Séquence crypto

1 Chiffre de César (20-30 minutes)

1. Introduction par des questions :
   - Savez-vous ce qu'est la cryptologie / cryptographie / cryptanalyse (/ stéganographie) ?
   - A quoi ça sert ?
   - De quand ça date ? César utilisait beaucoup les codes secrets. Il décrit dans ses "Commentaires sur la guerre des Gaules" (58 à 50 avant JC) l'usage d'un code qui est resté attaché à son nom : le *chiffre de César*.
2. *On distribue un disque à chiffrer à chaque membre du public, ainsi qu'une feuille "Chiffre de César", un stylo et un support. Avec l'applet, description du code de César* $a \to D$ *etc. La* clef *est D ou 3 (expliquer). Le destinataire du message doit avoir la clef pour le déchiffrer. On peut choisir d'autres décalages.* Pour vous simplifier la tâche, on vous donne des *disques à chiffrer* (inventés au XVe s. par Alberti). Vous choisissez un décalage, par exemple un décalage de 5 lettres $a \to F$ et vous positionnez les disques de sorte que le a et le F soient face à face. Ensuite vous transformez chaque lettre du message original en la lettre correspondante sur le disque intérieur. Pour vérifier que vous avez compris, chiffrer votre Prénom.
3. Un peu de vocabulaire : le chiffre de César est un *chiffre de substitution monoalphabétique*. Exemple de chiffre monoalphabétique plus général
4. Ces chiffres ont un gros défaut : ils sont vulnérables à *l'analyse de fréquences* (Première trace remonte à Al-Kindi, savant arabe du 9e siècle). Vous allez mettre en oeuvre cette analyse sur le message crypté sur la feuille que l'on vous a distribué. C'est un message chiffré par le chiffre de César. Comment feriez-vous pour le déchiffrer ?

5. Point crucial : toutes les lettres de l'alphabet n'ont pas la même *fréquence*. En français, le E est la lettre la plus fréquente. Cherchez la lettre la plus fréquente de votre texte, et voyez ce que ça donne si vous l'associez à un e. Si ça ne marche pas, vous pouvez essayer de la remplacer par un A, puis un I ou un S.
6. Conclusion : ce chiffre n'est vraiment pas sûr. Même si c'est un peu plus compliqué à mettre en oeuvre, un chiffre monoalphabétique général souffre du même défaut.
7. Il y a une autre façon de casser le chiffre de César : la *force brute*, 25 clefs possibles à essayer. Ceci est moins facile à mettre en oeuvre sur le chiffre monoalphabétique général : 26 !=4.032915e+26 clefs possibles.

2 Chiffre de subsitution monoalphabétique général (10-15 minutes)

Au lieu de faire juste un décalage, on permute aléatoirement les lettres de l'alphabet. Illustration avec l'applet "mono.jar" et le texte essai.txt. On a gardé la pnctuation pour rendre plus facile le décryptage. Après avoir identifié le e, utiliser le fait que le s est souvent en fin de mot, puis regarder les mots de deux lettres, de trois lettres etc.

3 Chiffre de Vigenère (20-30 minutes)

1. Une nouvelle possibilité apparut au XVe siècle sous la plume d'Alberti, et est passé à la postérité sous le titre de *chiffre de Vigenère*, du nom d'un diplomate qui l'utilisait. *Description de Vigenère avec l'applet.*
2. Ce chiffre a résisté longtemps, puis fut cassé par Charles Babbage au 19e siècle. Comment vous y prendriez-vous pour déchiffrer un message codé par Vigenère ? Indice : si vous connaissiez la longueur de la clef ?
3. A vous de jouer : pour que ça ne prenne pas trop de temps, on a déjà trouvé une partie de la clef sur vos textes. *Distribution des carrés de Vigenère et de la feuille "Chiffre de Vigenère"*
4. Et si on ne connait pas la longueur de la clef ? *Au tableau, description de la cryptanalyse de Vigenère, si le message est assez long par rapport à la clef.*

5. En conclusion, trop d'ordre nuit. Il existe une méthode absolument sûre, utilisant du désordre : la méthode du *masque jetable* (inventée par Frank Miller à la fin du 19e et réinventé par Mauborgne et Vernam au début du 20e siècle). On peut la voir comme un chiffre de Vigenère avec une clef aléatoire, de la longueur du message à chiffrer. *Au tableau, description du masque jetable.*

   Néanmoins, ce procédé pose un gros problème : celui de la distribution des clefs, d'autant qu'il en faut beaucoup !

4 Echange de clefs (10 minutes)

1. Jeu protocole : on prend trois membres du public, qu'on appellera Alice, Bob et Eve. Alice veut envoyer un message à Bob, et ce message passera par les mains d'Eve. Malheureusement, elle ne fait pas confiance à Eve, qui a tendance à être un peu trop curieuse et pourrait vouloir regarder le contenu du message d'Alice, qui est très secret. Eve et Bob possèdent chacun une pochette, un cadenas et des feuille de papier (représentant les messages possibles). Comment faire pour transmettre ce message en évitant qu'Eve en prenne connaissance ?

   Solution : Alice met son cadenas sur la pochette et envoie le message à Bob. Celui-ci met son cadenas et le renvoie à Alice. Celle-ci ôte son cadenas et renvoie sa pochette à Bob.

2. Plusieurs problèmes dans ce protocole :
   - Bob met un cadenas sur qqch dont il ne connait pas le contenu.
   - Il faut un aller-retour, ce n'est pas très pratique (exemple du mail).
   - Surtout, il y a un gros problème d'authentification : rien n'assure à Bob que le message vient bien d'Alice. Ce n'est robuste que face à un adversaire passif.

3. Eve dispose maintenant d'un cadenas. Comment peut-elle faire pour prendre connaissance du message échangé entre Alice et Bob ? Solution : elle met son cadenas sur la pochette d'Alice et lui renvoie, Alice enlève son cadenas et lui renvoie, Eve peut prendre connaissance du message. Elle envoie alors la pochette à Bob avec son cadenas accroché. Bob lui renvoie, elle enlève son cadenas. Remarquez qu'elle peut aussi changer le message d'Alice, initier toute seule une conversation avec Bob en faisant croire qu'elle est Alice etc.

4. Il y a un problème d'authentification. Comment faire ? Une solution simple : signer le message (en bas du message ou sur le message). Dans le monde numérique, ce n'est pas si facile, mais les mathématiques premettent de faire cela.

5 Crypto à clef publique et fonctions à sens unique.

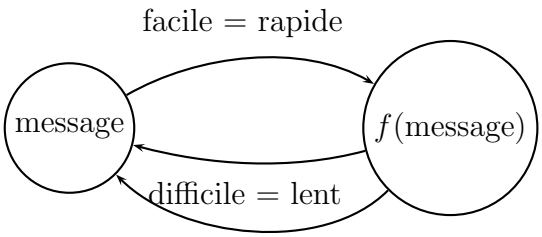
Cette partie n'est pas à mettre en oeuvre devant un groupe, mais peut servir avec un public motivé de 1 à 3 personnes. Selon la formation de l'interlocuteur

1. Un autre système pour éviter les aller-retours de cadenas : la crypto à clef publique. Besoin d'une quatrième personne : le tiers de confiance (celui qui tient le stand). Celui-ci donne, à la demande des copies du cadenas d'Alice, dont seule Alice a la clef. De même le Tiers de confiance peut donner des copies du cadenas de Bob. Pour envoyer un message à Bob, Alice demande au tiers de confiance un cadenas de Bob puis envoie son message à Bob avec ce cadenas dessus. De même si Bob veut répondre, il utilise un cadenas d'Alice. Il y a toujours le problème d'authentification. Comment faire ? Une solution simple : signer le message (en bas du message ou sur le message). Dans le monde numérique, ce n'est pas si facile.
2. Les mathématiques ont donné naissance à des *fonctions à sens unique*, qu'on utilise comme des fonctions de chiffrement publique.
3. Dans le monde numérique,

Tableau:
message $\leftrightarrow$ nombre
chiffrer un message $\leftrightarrow$ appliquer une fonction au nombre
cadenas $\leftrightarrow$ fonction à sens unique
clef (secrète) $\leftrightarrow$ brèche secrète dans la fonction à sens unique

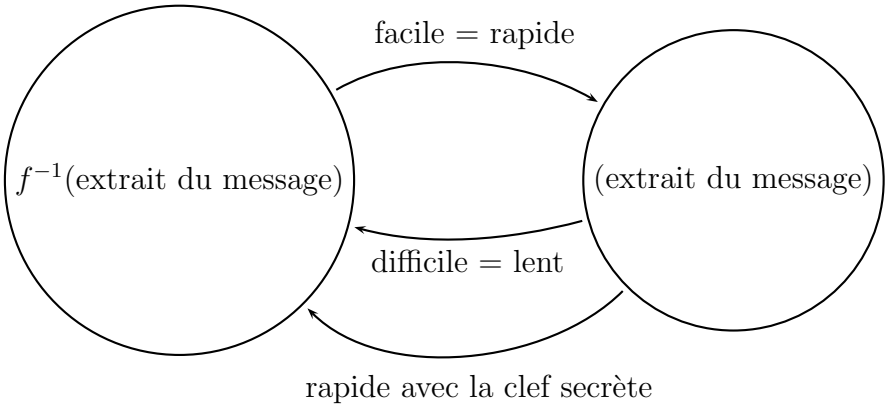
Les mathématiques permettent de trouver des fonctions à sens unique :

Elle permet aussi de signer en prouvant qu'on sait faire quelque chose



rapide avec la clef secrète

qui serait très difficile à faire pour une personne ne connaissant pas la clef secrète :



Remarque : il faut utiliser un extrait de message qui est lui-même l'image du message par une fonction à sens unique.

4. Nous allons décrire une fonction à sens unique : l'*exponentielle discrète*, qui est à la base de l'*échange de clefs de Diffie-Hellman*.
5. Cela fait appel à ce qu'on pourrait appeler l'arithmétique de l'horloge. *Explication au tableau.* Prenons une horloge avec seulement l'aiguille des heures, et essayons d'ajouter deux nombres. Disons qu'il est 10h du matin, vous lancez un gros téléchargement sur internet qui doit durer 4 heures. Au bout de quatre heures, l'aiguille de l'horloge sera sur le nombre 2. L'horloge aura "oublié" le tour qu'elle a fait. Elle aura d'elle-même soustrait douze heures au résultat. On dit que $10+4 = 2$ modulo 12. Au lieu d'ajouter deux nombres, on peut multiplier deux nombres. Par exemple, $5 * 3 = 3$ modulo 12.

6. Cette propriété de repliement peut sembler sympathique, mais en fait, elle rend très compliquée certaines opérations. Prenons un entier, par exemple 5, que nous allons multiplier par lui-même de manière répétée. Nous allons comparer la façon dont ça se passe dans l'arithmétique classique, celle que tout lemonde utilise tous les jours, et dans l'arithmétique de l'horloge, qu'on appelle en fait arithmétique modulaire. Tout d'abord, dans l'arithmétique classique, on obtient $5, 25, 125, 625, 3125, 15625, 78125, 390625$ etc. Dans l'arithmétique modulaire modulo 17, on obtient : $5, 8, 6, 13, 14, 2, 10, 16$. L'ordre est chamboulé, et les écarts successifs ne semblent pas avoir de régularité particulière. Lorsqu'on remplace 17 par un très grand nombre premier p, et que g est un nombre entre 1 et $p-2$ (en fait un générateur du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z}^*)$, la fonction qui à x associe g^x est une fonction à sens unique : il est très difficile de retrouver x lorsqu'on ne connait que g^x. Essentiellement, aujourd'hui, pour inverser cette fonction il faut calculer successivement les puissances de g jusqu'à trouver la bonne valeur. Cela prend en moyenne de l'ordre de p multiplications. Par contre, pour calculer g^x, il suffit en moyenne d'utiliser de l'ordre de $\log(p)$ multiplications. On peut donc choisir la taille de p pour que p soit gigantesque par rapport à $\log(p)$. Le temps de calcul de g^x sera alors court, et le temps de l'inversion prohibitif (aujourd'hui, les nombres premiers utilisés ont plusieurs centianes de chiffres).

7. *Description de Diffie-Hellman.* On va voir comment on peut alors utiliser cette fonction à sens unique pour résoudre le problème du *partage de clefs*. Alice veut convenir avec Bob d'une clef secrète, mais savent que Eve peut écouter le message. Alice choisit un grand nombre premier p, puis un nombre g au hasard entre 1 et $p-1$. Elle communique g et p à Bob en clair. Puis elle choisit a au hasard entre 1 et $p-2$ et transmet g^a à Bernard. Bernard fait la même chose de son côté : il choisit un nombre b au hasard entre 1 et $p-2$ et transmet g^b à Alice. Maintenant, Alice calcule g^{ab} en élevant g^b à la puissance a. Bob calcule g^{ab} en élevant g^a à la puissance b. Eve, elle , connait g, p, g^a, g^b mais ne connait ni a ni b et ne peut les trouver facilement car la fonction qui à x associe g^x est une fonction à sens unique.

8. Description de El Gamal : le message est transformé en un nombre entre 1 et $p-1$ selon une règle connue de tous. Ensuite, on procède comme dans Diffie-Hellman, et le cryptage consiste à multiplier (modulo p) le message par la clef de Diffie-Hellman. En fait, on le formule usuellement

comme un algo de cryptage à clef publique : la clef publique d'Alice est (p, g, g^a) et sa clef privée est a. Puis, chaque fois que Bob veut envoyer un message m à Alice, il choisit un nombre b au hasard comme ci-dessus et transmet à Alice $(g^b, g^{ab}m)$. Alice peut alors calculer g^{ab} et déchiffrer $g^{ab}m$.